Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Adventia Chat Cross-Site Scripting Vulnerabilities
  - Bugtracker.NET Unspecified SQL Injection Vulnerabilities
  - Cerulean Studios Trillian Remote Code Execution Vulnerability
  - M. Dev Software ZipGenius Remote File Creation Vulnerability
  - Microsoft Outlook 2002 Connector For IBM Lotus Domino Policy Bypass Vulnerability
  - Microsoft Windows Remote Desktop 'TSShutdn.exe' Denial of Service Vulnerability
  - Mysoft Technology Maxthon "m2_search_text" Information Disclosure Vulnerability
  - Nortel Contivity VPN Client Password Disclosure Vulnerability
  - Symantec Multiple Products AutoProtect Errors Denial of Service Vulnerability
  - Uapplication Ublog Cross-Site Scripting Vulnerability
  - Ubisoft The Settlers: Heritage of Kings Player Logging Buffer Overflow Vulnerability
- UNIX / Linux Operating Systems
  - **Apple Safari IDN Implementation URL Spoof (Updated)**
  - **Carnegie Mellon University Cyrus IMAP Server Multiple Remote Buffer Overflows (Updated)**
  - Dnsmasq Multiple Remote Vulnerabilities
  - ESMI PayPal Storefront SQL Injection & Cross-Site Scripting
  - **Ethereal Multiple Dissector Vulnerabilities (Updated)**
  - **GNU Sharutils Multiple Buffer Overflow (Updated)**
  - Greg Woods Smail-3 Multiple Remote and Local Vulnerabilities
  - **Grip CDDB Query Buffer Overflow (Updated)**
  - ImageMagick Multiple Remote Vulnerabilities
  - J. Shilling CDRTools CDRecord Insecure File Creation
  - **KDE DCOPServer Local Denial of Service (Updated)**
  - **KDE 'DCOPIDLING' Library (Updated)**
  - **LibEXIF Library EXIF Tag Structure Validation (Updated)**
  - Mathopd Dump Files Insecure File Creation
  - Midnight Commander 'Insert_Text' Buffer Overflow
  - **Mozilla Firefox Predictable Plugin Temporary Directory (Updated)**
  - **Multiple Vendors Clam Anti-Virus ClamAV Remote Denial of Service (Updated)**
  - **Multiple Vendors GNU Exim Buffer Overflows (Updated)**
  - **Multiple Vendors ImageMagick File Name Handling Remote Format String (Updated)**
  - **Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel Terminal Locking Race Condition (Updated)**
  - **Multiple Vendors Linux Kernel TIOCSETD Terminal Subsystem Race Condition (Updated)**
  - **Multiple Vendors Evolution Camel-Lock-Helper Application Remote Buffer Overflow (Updated)**
  - **Multiple Vendors MySQL Database Unauthorized GRANT Privilege (Updated)**
  - Multiple Vendors Sylpheed MIME-Encoded Attachment Name Buffer Overflow
  - Multiple Vendors Apache mod_ssl 'ssl_io_filter_cleanup' Remote Denial of Service
  - **Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows (Updated)**
  - **Multiple Vendors KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Moxa Char Driver Buffer Overflows (Updated)**
  - **Multiple Vendors Linux Kernel Overlapping VMAs (Updated)**
  - Multiple Vendors Linux Kernel Bluetooth Signed Buffer Index
  - **Multiple Vendors Linux Kernel Netfilter Memory Leak Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Local Buffer Overflows & Information Disclosure (Updated)**
  - Multiple Vendors Linux Kernel Local Denial of Service
  - **Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - Multiple Vendors Linux Kernel EXT2 File System Information Leak
  - **Multiple Vendors Linux Kernel ReiserFS File System Local Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel SYS_EPoll_Wait Elevated Privileges (Updated)**

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adventia Adventia Chat 3.1, Adventia Chat Server Pro 3.0	A vulnerability has been reported that could let a remote user conduct Cross-Site Scripting attacks. This is because the server permits users to submit HTML code into chat sessions by default. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Adventia Chat Cross-Site Scripting Vulnerabilities CAN-2005-0919	High	Security Focus, Bugtraq ID 12927, March 29, 2005
Bugtracker.NET Bugtracker.NET 2.0.1	A vulnerability was reported that could let a remote malicious user conduct SQL Injection attacks. A fixed version (2.0.2) is available: http://prdownloads.sourceforge.net/btnet/btnet_2_0_2.zip?download No exploit is required.	Bugtracker.NET Unspecified SQL Injection Vulnerabilities CAN-2005-0920	High	Security Focus, Bugtraq ID 12925, March 29, 2005
Cerulean Studios Trillian 2.0, 3.0 and 3.1	A buffer overflow vulnerability was reported in processing HTTP 1.1 response headers that could let a remote server execute arbitrary code. The AIM, Yahoo, MSN, and RSS plugins are affected. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Cerulean Studios Trillian Remote Code Execution Vulnerability CAN-2005-0874 CAN-2005-0875	High	LogicLibrary BugScan Vulnerability Summary Report Trillian 2.0, 3.0 and 3.1, March 23, 2005
M.Dev Software ZipGenius 5.5	A directory traversal vulnerability was reported that could let a remote malicious user create a zip file that, when uncompressed, will create files in arbitrary directories on the target system. This is because of filenames in zip archives are not properly validated. A fixed version (6 Beta) is available: http://www.zipgenius.it A Proof of Concept exploit has been published.	M. Dev Software ZipGenius Remote File Creation Vulnerability CAN-2005-0329	Medium	Security Tracker Alert ID: 1013542, March 24, 2005
Microsoft Outlook 2002 Connector For IBM Lotus Domino	A vulnerability has been reported that could let a malicious user bypass policy. This is because the application saves login credentials locally even when a Group policy is in place to prevent this. A hotfix is available: http://support.microsoft.com/kb/888991 No exploit is required.	Microsoft Outlook 2002 Connector For IBM Lotus Domino Policy Bypass Vulnerability CAN-2005-0921	Medium	Security Focus, Bugtraq ID 12913, March 28, 2005
Microsoft Windows XP SP1	A vulnerability was reported that could let a remote authenticated malicious user cause a Denial of Service. This is because of improper validation during the 'Force shutdown from a remote system' process. A solution is available: http://support.microsoft.com/kb/889323/ A Proof of Concept exploit has been published.	Microsoft Windows Remote Desktop 'TSShutdn.exe' Denial of Service Vulnerability CAN-2005-0904	Low	Security Tracker Alert ID: 1013552, March 24, 2005
Mysoft Technology Maxthon (MyIE2) 1.2.0	A vulnerability was reported that could let malicious users access potentially sensitive information. This is due to an error in the API for plug-ins where search bar data is not properly protected. Update to version 1.2.1: http://www.maxthon.com/download.htm A Proof of Concept exploit has been published.	Mysoft Technology Maxthon "m2_search_text" Information Disclosure Vulnerability CAN-2005-0905	Medium	Secunia SA14712, March 28, 2005

Nortel Nortel Contivity VPN Client 5.01	A vulnerability has been reported that could let a local malicious user obtain the password. This is because of the way the VPN client software stores the VPN password in process memory. A local user with access to the 'Extranet.exe' process memory can recover the user or group password. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Nortel Contivity VPN Client Password Disclosure Vulnerability CAN-2005-0844	High	Security Tracker Alert ID: 1013512, March 22, 2005
Symantec Norton System Works 2004 and 2005, Norton Internet Security 2004 and 2005, Norton AntiVirus 2004 and 2005	Two vulnerabilities were reported in the AutoProtect feature that could let a malicious user create a file or modify a filename to cause a Denial of Service. A user can create a special file of a specific file type that when scanned by the AutoProtect feature will cause a Denial of Service. Also, if a certain type of shared file has its filename modified, the SmartScan analysis of the filename modification may cause a Denial of Service. A fix is available via LiveUpdate. Currently we are not aware of any exploits for these vulnerabilities.	Symantec Multiple Products AutoProtect Errors Denial of Service Vulnerability CAN-2005-0922 CAN-2005-0923	Low	Symantec Advisory, SYM05-006 March 28, 2005
Uapplication Ublog 1.0, 1.0.3, 1.0.4	A vulnerability has been reported that could let a remote malicious user conduct Cross-Site Scripting attacks. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Uapplication Ublog Cross-Site Scripting Vulnerability CAN-2005-0925	High	Security Focus, Bugtraq ID 12931, March 29, 2005
Ubisoft The Settlers: Heritage of Kings 1.02 and prior	A buffer overflow vulnerability was reported that could let a remote malicious user compromise a vulnerable system. Upgrade to Version 1.03. A Proof of Concept exploit has been published.	Ubisoft The Settlers: Heritage of Kings Player Logging Buffer Overflow Vulnerability CAN-2005-0906	Not Specified	Secunia SA14762, March 29, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apple Safari 1.2.5	A vulnerability exists when processing International Domain Names (IDNs), which could let a remote malicious user spoof web sites. **Update available at:** **http://docs.info.apple.com/article.html?artnum=301061** A Proof of Concept exploit has been published.	Apple Safari IDN Implementation URL Spoof CAN-2005-0234	Medium	Secunia Advisory, SA14164, February 7, 2005 **US-CERT VU#273262**
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200502-29.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva:	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 2005 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:009, February 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:051, March 4, 2005 Conectiva Linux Security Announcement, CLA-2005:937, March 17, 2005 **ALTLinux Security Advisory, March 29, 2005**

	ftp://atualizacoes.conectiva.com.br/ **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for these vulnerabilities.			
Dnsmasq Dnsmasq 2.0-2.20	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to an off-by-one error when reading the DHCP lease file, which could let a remote malicious user cause a Denial of Service; and a vulnerability has been reported when receiving DNS replies due to insufficient validation, which could let a remote malicious user poison the DNS cache. Upgrades available at: http://www.thekelleys.org.uk/dnsmasq/dnsmasq-2.21.tar.gz Currently we are not aware of any exploits for these vulnerabilities.	Dnsmasq Multiple Remote Vulnerabilities CAN-2005-0876 CAN-2005-0877	Low/ Medium (Medium if the DNS cache can be poisoned)	Security Focus, 12897, March 25, 2005
Esmistudio.com PayPal Storefront 1.7	Multiple vulnerabilities have been reported: a vulnerability has been reported in the 'pages.php' and 'products1.php' scripts due to insufficient validation of user-supplied data, which could let a remote malicious user execute arbitrary SQL commands; and a Cross-Site Scripting vulnerability has been reported in the 'products1h.php' script due to insufficient validation of the 'id' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	ESMI PayPal Storefront SQL Injection & Cross-Site Scripting CAN-2005-0935 CAN-2005-0936	High	Dcrab 's Security Advisory, March 25, 2005
Ethereal Group Ethereal 0.8, 0.8.13-0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.8	Multiple vulnerabilities exist: remote Denial of Service vulnerabilities exist in the COPS, DLSw, DNP, Gnutella, and MMSE dissectors; and a buffer overflow vulnerability exists in the X11 dissector, which could let a remote malicious user execute arbitrary code. Ethereal: http://www.ethereal.com/download.html Debian: http://security.debian.org/pool/updates/main/e/ethereal/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-27.xml SuSE: ftp://ftp.suse.com/pub/suse/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Dissector Vulnerabilities CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084	Low/High (High if arbitrary code can be executed)	Security Tracker Alert, 1012962, January 21, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 **Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005** **ALTLinux Security Advisory, March 29, 2005**
GNU sharutils 4.2, 4.2.1	Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-01.xml **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** **Ubuntu:**	GNU Sharutils Multiple Buffer Overflow CAN-2004-1773	Low/High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004 **Fedora Legacy Update Advisory, FLSA:2155, March 24, 2005** **Ubuntu Security Notice, USN-102-1 March 29, 2005**

	http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ We are not aware of any exploits for this vulnerability.			
Greg A. Woods Smail-3 3.2.0.120	Multiple vulnerabilities have been reported: a vulnerability has been reported in 'addr.c' due to a heap overflow, which could let a remote malicious user execute arbitrary code with root privileges; and a vulnerability has been reported in 'modes.c' due to insecure handling of heap memory by signal handlers, which could let a malicious user execute arbitrary code with root privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Smail-3 Multiple Remote and Local Vulnerabilities CAN-2005-0892 CAN-2005-0893	High	Security Tracker Alert, 1013564, March 27, 2005
Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200503-21.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-304.html** Currently we are not aware of any exploits for this vulnerability.	Grip CDDB Query Buffer Overflow CAN-2005-0706	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005 Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005 **RedHat Security Advisory, RHSA-2005:304-08, March 28, 2005**
ImageMagick ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0 , 5.4.8, 5.5.3 .2-1.2.0, 5.5.4, 5.5.6 .0-20030409, 5.5.6, 5.5.7, 6.0, 6.0.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported in the decoder due to a failure to handle malformed TIFF tags; a remote Denial of Service vulnerability has been reported due to a failure to handle malformed TIFF images; a remote Denial of Service vulnerability has been reported due to a failure to handle malformed PSD files; and a buffer overflow vulnerability has been reported in the SGI parser, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.imagemagick.org/script/download.php? SuSE: ftp://ftp.suse.com/pub/suse RedHat: http://rhn.redhat.com/errata/RHSA-2005-070.html Currently we are not aware of any exploits for these vulnerabilities.	ImageMagick Multiple Remote Vulnerabilities CAN-2005-0759 CAN-2005-0760 CAN-2005-0761 CAN-2005-0762	Low/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013550, March 24, 2005
J. Schilling CDRTools 2.0	A vulnerability has been reported in cdrecord due to insecure creation of various files, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cdrtools/ There is no exploit code required.	CDRTools CDRecord Insecure File Creation CAN-2005-0866	Medium	Ubuntu Security Notice USN-100-1, March 24, 2005

KDE KDE 1.1-1.1.2, 1.2, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2	A Denial of Service vulnerability has been reported in the Desktop Communication Protocol (DCOP) daemon due to an error in the authentication process Upgrade available at: http://www.kde.org/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-22.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-325.html** **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	KDE DCOPServer Local Denial of Service CAN-2005-0396	Low	KDE Security Advisory, March 16, 2005 **Fedora Update Notifications, FEDORA-2005-244 & 245, March 23, 2005** **RedHat Security Advisory, RHSA-2005:325-07, March 23, 2005** **ALTLinux Security Advisory, March 29, 2005**
KDE kdelibs 3.3.2	A vulnerability exists in the 'dcopidling' library due to insufficient validation of a files existence, which could let a malicious user corrupt arbitrary files. Patch available at: http://bugs.kde.org/attachment.cgi?id=9205&action=view Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-14.xml **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-325.html** **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	KDE 'DCOPIDLING' Library CAN-2005-0365	Medium	Security Focus, February 11, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:045, February 18, 2005 Gentoo Linux Security Advisory, GLSA 200503-14, March 7, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:058, March 16, 2005 **Fedora Update Notifications, FEDORA-2005-244 & 245, March 23, 2005** **RedHat Security Advisory, RHSA-2005:325-07, March 23, 2005** **ALTLinux Security Advisory, March 29, 2005**
libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-17.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-300.html** Currently we are not aware of any exploits for this vulnerability.	LibEXIF Library EXIF Tag Structure Validation CAN-2005-0664	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update Notifications, FEDORA-2005-199 & 200, March 8, 2005 Gentoo Linux Security Advisory, GLSA 200503-17, March 12, 2005 **RedHat Security Advisory, RHSA-2005:300-08, March 21, 2005**
Mathopd Mathopd Web Server 1.5 p4, 1.6 b5	A vulnerability has been reported in the 'internal_dump()' function due to the insecure creation of dump files when a SIGWINCH signal is caught, which could let a malicious user corrupt arbitrary files.	Mathopd Dump Files Insecure File Creation	Medium	Secunia Advisory, SA14524, March 23, 2005

	Upgrades available at: http://www.mathopd.org/dist/mathopd-1.5p5.tar.gz There is no exploit code required.	CAN-2005-0824		
Midnight Commander Midnight Commander 4.5.40-4.5.5.52, 4.5.54, 4.5.55	A buffer overflow vulnerability has been reported in the 'insert_text()' function due to insufficient bounds checking, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ Currently we are not aware of any exploits for this vulnerability.	Midnight Commander 'Insert_Text' Buffer Overflow CAN-2005-0763	High	Debian Security Advisory, DSA 698-1 , March 29, 2005
Mozilla.org Firefox 1.0	A vulnerability exists because a predictable name issued for the plugin temporary directory, which could let a malicious user cause a Denial of Service or modify system/user information. Update available at: http://www.mozilla.org/products/firefox/all.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-10.xml SuSE: ftp://ftp.suse.com/pub/suse/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml** **http://security.gentoo.org/glsa/glsa-200503-32.xml** An exploit has been published.	Mozilla Firefox Predictable Plugin Temporary Directory CAN-2005-0578	Low/ Medium (Medium if user/system information can be modified)	Mozilla Foundation Security Advisory, 2005-28, February 25, 2005 SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005 **Fedora Update Notification, FEDORA-2005-247 2005-03-23** **Gentoo Linux Security Advisory, GLSA 200503-30 & GLSA 200503-032, March 25, 2005**
Multiple Vendors ClamAV 0.51-0.54, 0.60, 0.65, 0.67, 0.68 -1, 0.68, 0.70, 0.80 rc1-rc4, 0.80; MandrakeSoft Corporate Server 3.0 x86_64, 3.0. Linux Mandrake 10.1 X86_64, 10.1	A remote Denial of Service vulnerability exists due to an error in the handling of file information in corrupted ZIP files. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=300116 Gentoo: http://security.gentoo.org/glsa/glsa-200501-46.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://www.trustix.org/errata/2005/0003/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/RPMS/libclamav-devel-static-0.83-70136U10_7cl.i386.rpm **ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	Clam Anti-Virus ClamAV Remote Denial of Service CAN-2005-0133	Low	Security Focus, January 31, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:025, January 31, 2005 Gentoo Linux Security Advisory, GLSA 200501-46, January 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Conectiva Linux Security Announcement, CLA-2005:928, March 3, 2005 **ALTLinux Security Advisory, March 29, 2005**

Multiple Vendors Exim 4.43 & prior	Multiple vulnerabilities exist that could allow a local user to obtain elevated privileges. There are buffer overflows in the host_aton() function and the spa_base64_to_bits() functions. It may be possible to execute arbitrary code with the privileges of the Exim process. The vendor has issued a fix in the latest snapshot: ftp://ftp.csx.cam.ac.uk/pub/software/email/exim/ Testing/exim-snapshot.tar.gz ftp://ftp.csx.cam.ac.uk/pub/software/email/exim/Testing/exim-snapshot.tar.gz.sig Also, patches for 4.43 are available at: http://www.exim.org/mail-archives/exim-announce/2005/msg00000.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/exim4/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-23.xml Debian: http://security.debian.org/pool/updates/main/e/exim/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** An exploit script has been published.	GNU Exim Buffer Overflows CAN-2005-0021 CAN-2005-0022	High	Security Tracker Alert ID: 1012771, January 5, 2005 Gentoo Linux Security Advisory, GLSA 200501-23, January 12, 2005 Debian Security Advisory, DSA 635-1 & 637-1, January 12 & 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 US-CERT Vulnerability Note, VU#132992, January 28, 2005 Security Focus, February 12, 2005 **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors ImageMagick 5.3.3, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0-6.0.8, 6.1-6.1.7, 6.2	A format string vulnerability exists when handling malformed file names, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Update available at: http://www.imagemagick.org/script/downloads.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-11.xml **SUSE: ftp://ftp.suse.com/pub/suse/** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-320.html** Currently we are not aware of any exploits for this vulnerability.	ImageMagick File Name Handling Remote Format String CAN-2005-0397	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14466, March 4, 2005 Ubuntu Security Notice, USN-90-1, March 3, 2004 **SUSE Security Announcement, SUSE-SA:2005:017, March 23, 2005** **RedHat Security Advisory, RHSA-2005:320-10, March 23, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005 **Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005**
Multiple Vendors Linux Kernel versions except 2.6.9	A race condition vulnerability exists in the Linux Kernel terminal subsystem. This issue is related to terminal locking and is exposed when a remote malicious user connects to the computer through a PPP dialup port. When the remote user issues the switch from console to PPP, there is a small window of opportunity to send data that will trigger the vulnerability. This may cause a Denial of Service.	Multiple Vendors Linux Kernel Terminal Locking Race Condition CAN-2004-0814	Low	Security Focus, December 14, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005

	This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Mandrake: http://www.mandrakesecure.net/en/ftp.php FedoraLegacy: http://download.fedoralegacy.org/redhat/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005 Turbolinux Security Announcement , February 28, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005**
Multiple Vendors Linux Kernel versions except 2.6.9	The Linux Kernel is prone to a local vulnerability in the terminal subsystem. Reportedly, this issue can be triggered by issuing a TIOCSETD ioctl to a terminal interface at the moment a read or write operation is being performed by another thread. This could result in a Denial of Service or allow kernel memory to be read. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Mandrake: http://www.mandrakesecure.net/en/ftp.php FedoraLegacy: http://download.fedoralegacy.org/redhat/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel TIOCSETD Terminal Subsystem Race Condition CAN-2004-0814	Low	Security Focus, December 14, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005**
Multiple Vendors MandrakeSoft Corporate Server 3.0, x86_64, Linux Mandrake 10.0, AMD64, 10.1, X86_64;Novell Evolution 2.0.2l Ubuntu Linux 4.1 ppc, ia64, ia32; Ximian Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.4, 1.3.2 (beta)	A buffer overflow vulnerability exists in the main() function of the 'camel-lock-helper.c' source file, which could let a remote malicious user execute arbitrary code. Update available at: http://cvs.gnome.org/viewcvs/evolution/camel/camel-lock-helper.c?rev=1.7&hideattic=0&view=log Gentoo: http://security.gentoo.org/glsa/glsa-200501-35.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/e/evolution/ Conectiva: ftp://atualizacoes.conectiva.com.br/	Evolution Camel-Lock-Helper Application Remote Buffer Overflow CAN-2005-0102	High	Gentoo Linux Security Advisory, GLSA 200501-35, January 25, 2005 Ubuntu Security Notice, USN-69-1, January 25, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:024, January 27, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Debian Security Advisory, DSA 673-1, February 10, 2005 Conectiva Linux Security Announcement, CLA-2005:925, February 16, 2005 **ALTLinux Security Advisory, March 29, 2005**

	ALT Linux: **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors MySQL AB MySQL 3.20.x, 3.20.32 a, 3.21.x, 3.22.x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.54, 3.23.56, 3.23.58, 3.23.59, 4.0.0-4.0.15, 4.0.18, 4.0.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0, 2.1	A vulnerability exists in the 'GRANT' command due to a failure to ensure sufficient privileges, which could let a malicious user obtain unauthorized access. Upgrades available at: http://dev.mysql.com/downloads/mysql/4.0.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2004-611.html SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/m Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** There is no exploit code required.	MySQL Database Unauthorized GRANT Privilege CAN-2004-0957	Medium	Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 **Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005**
Multiple Vendors RedHat Fedora Core3 & Core 2; Sylpheed Sylpheed 0.8, 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0 .0-1.0.3, 1.9-1.9.4	A buffer overflow vulnerability has been reported when handling email messages that contain attachments with MIME-encoded file names, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sylpheed: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.4.tar.gz Currently we are not aware of any exploits for this vulnerability.	Sylpheed MIME-Encoded Attachment Name Buffer Overflow CAN-2005-0926	High	Fedora Update Notifications, FEDORA-2005-263 & 264, March 29, 2005
Multiple Vendors Apache Software Foundation Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.49; SuSE Secure Linux 2.1, 8.2, 9.0 x86_64m 9.0, 9.1 x86_64, 9.1, Linux Enterprise Server 9	A remote Denial of Service vulnerability has been reported in the 'ssl_io_filter_cleanup' function. Upgrades available at: http://httpd.apache.org/download.cgi SuSE: ftp://ftp.suse.com/pub/suse There is no exploit code required.	Apache mod_ssl 'ssl_io_filter_cleanup' Remote Denial of Service	Low	Security Focus, 12877, March 23, 2005

Multiple Vendors Daniel Stenberg curl 6.0-6.4, 6.5-6.5.2, 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.7, 7.12.1	A buffer overflow vulnerability exists in the Kerberos authentication code in the 'Curl_krb_kauth()' and 'krb4_auth()' functions and in the NT Lan Manager (NTLM) authentication in the 'Curl_input_ntlm()' function, which could let a remote malicious user execute arbitrary code. SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Updates available at: http://curl.haxx.se/download/curl-7.13.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200503-20.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows CAN-2005-0490	High	iDEFENSE Security Advisory , February 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:048, March 4, 2005 Gentoo Linux Security Advisory, GLSA 200503-20, March 16, 2005 Conectiva Linux Security Announcement, CLA-2005:940, March 21, 2005 **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors IPsec-Tools IPsec-Tools 0.5; KAME Racoon prior to 20050307	A remote Denial of Service vulnerability has been reported when parsing ISAKMP headers. Upgrades available at: http://www.kame.net/snap-users/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-232.html** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-30.xml** **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service CAN-2005-0398	Low	Fedora Update Notifications, FEDORA-2005-216 & 217, March 14, 2005 **RedHat Security Advisory, RHSA-2005:232-10, March 23, 2005** **Gentoo Linux Security Advisory, GLSA 200503-33, March 25, 2005** **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors Linux Kernel 2.2, 2.4, 2.6	Several buffer overflow vulnerabilities exist in 'drivers/char/moxa.c' due to insufficient validation of user-supplied inputs to the 'MoxaDriverloctl(),' ' moxaloadbios(),' moxaloadcode(),' and 'moxaload320b()' functions, which could let a malicious user execute arbitrary code with root privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/l **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Moxa Char Driver Buffer Overflows CAN-2005-0504	High	Security Tracker Alert, 1013273, February 23, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005**

Multiple Vendors Linux kernel 2.4.0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2	A vulnerability exists in the processing of ELF binaries on IA64 systems due to improper checking of overlapping virtual memory address allocations, which could let a malicious user cause a Denial of Service or potentially obtain root privileges. Patch available at: http://linux.bkbits.net:8080/linux-2.6/cset@41a6721cce-LoPqkzKXudYby_3TUmg Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-043.html http://rhn.redhat.com/errata/RHSA-2005-017.html Mandrake: http://www.mandrakesecure.net/en/ftp.php TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Overlapping VMAs CAN-2005-0003	Low/High (High if root access can be obtained)	Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 RedHat Security Advisories, RHSA-2005:043-13 & RHSA-2005:017-14m January 18 & 21, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 Turbolinux Security Announcement , February 28, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005**
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ A Proof of Concept exploit script has been published.	Linux Kernel Bluetooth Signed Buffer Index CAN-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005
Multiple Vendors Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Netfilter Memory Leak Denial of Service CAN-2005-0210	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005** **Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005**

Multiple Vendors Linux kernel 2.6 .10, 2.6-2.6.11	Multiple vulnerabilities exist: a vulnerability exists in the 'radeon' driver due to a race condition, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the 'i2c-viapro' driver, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'locks_read_proc()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in 'drivers/char/n_tty.c' due to a signedness error, which could let a malicious user obtain sensitive information; and potential errors exist in the 'atm_get_addr()' function and the 'reiserfs_copy_from_user_to_file_region()' function. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.11-rc4.bz2 SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Exploit scripts have been published.	Linux Kernel Multiple Local Buffer Overflows & Information Disclosure **CAN-2005-0529** **CAN-2005-0530** **CAN-2005-0531** **CAN-2005-0532**	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14270, February 15, 2005 Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005** **Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005** **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Local Denial of Service CAN-2005-0749	Low	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol (PPP) Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Trustix: http://http.trustix.org/pub/trustix/updates **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005** **Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005** **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1--test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **SUSE Security**

	RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** Currently we are not aware of any exploits for these vulnerabilities.			**Announcement, SUSE-SA:2005:018, March 24, 2005** **Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1-2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005
Multiple Vendors Linux kernel 2.6.8 rc1-rc3	A Denial of Service vulnerability exists in the 'ReiserFS' file system functionality due to a failure to properly handle files under certain conditions. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrake: http://www.mandrakesecure.net/en/ftp.php TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	Multiple Vendors Linux Kernel ReiserFS File System Local Denial of Service CAN-2004-0814	Low	Security Focus, October 26, 2004 Ubuntu Linux Security Advisory USN-38-1, December 14, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005**
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in 'SYS_EPoll_Wait' due to a failure to properly handle user-supplied size values, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** An exploit script has been published.	Linux Kernel SYS_EPoll_Wait Elevated Privileges CAN-2005-0736	Medium	Security Focus, 12763, March 8, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 Security Focus, 12763, March 22, 2005 **Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005**

Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 **Ubuntu Security Notice, USN-97-1 March 16, 2005** **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors xli 1.14-1.17	A vulnerability exists due to a failure to manage internal buffers securely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	XLI Internal Buffer Management CAN-2005-0639	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **ALTLinux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for this vulnerability.	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 **ALTLinux Security Advisory, March 29, 2005**

MySQL AB Conectiva Debian Engarde FreeBSD Gentoo HP IBM Immunix Mandrake OpenBSD OpenPKG RedHat Trustix Sun SuSE MySQL AB MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2-3.23.5, 3.23.8- 3.23.10, 3.23.22- 3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0 .0-4.0.15, 4.0.18, 4.1.0-0, 4.1 .0-alpha	A vulnerability exists in the MySQL 'mysqld_multi' script due to insecure temporary file handling, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/mysql/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/mysql-4.0.18-2.0.1.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200405-20.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** There is not exploit code required.	MySQL 'mysqld_multi' Insecure Temporary File Handling CAN-2004-0388	Medium	Debian Security Advisory, DSA 483-1, April 14, 2004 Gentoo Linux Security Advisory, GLSA 200405-20, May 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:034, April 20, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.014, April 14, 2004 Turbolinux Security Announcement, February 17, 2005 **Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005**
MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21 .x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0.0-4.0.15, 4.0.18, 4.0.20, 4.1 .0-alpha, 4.1 .0-0, 4.1.2 -alpha, 4.1.3 -beta, 4.1.3 -0, 5.0 .0-alpha, 5.0 .0-0	A buffer overflow vulnerability exists in the 'mysql_real_connect' function due to insufficient boundary checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. *Note: Computers using glibc on Linux and BSD platforms may not be vulnerable to this issue.* Debian: http://security.debian.org/pool/updates/main/m/mysql/ Trustix: http://http.trustix.org/pub/trustix/updates/ OpenPKG: ftp://ftp.openpkg.org/release/ Mandrake: http://www.mandrakesoft.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.suse.com/pub/suse Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** We are not aware of any exploits for this vulnerability.	MySQL Mysql_real_connect Function Remote Buffer Overflow CAN-2004-0836	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA12305, August 20, 2004 Debian Security Advisory, DSA 562-1, October 11, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:892, November 18, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 **Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005**
MySQL AB MySQL 3.23.49, 4.0.20	A vulnerability exists in the 'mysqlhotcopy' script due to predictable files names of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-02.xml SuSE:	MySQL 'Mysqlhotcopy' Script Elevated Privileges CAN-2004-0457	Medium	Debian Security Advisory, DSA 540-1, August 18, 2004 Gentoo Linux Security Advisory GLSA 200409-02, September 1, 2004 SUSE Security Announcement, SUSE-SA:2004:030, September 6, 2004

	ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-569.html OpenPKG: ftp://ftp.openpkg.org/release/ Mandrake: http://www.mandrakesoft.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** There is no exploit code required.			RedHat Security Advisory, ,RHSA-2004:569-16, October 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004 SUSE Security Summary Report, USE-SR:2004:001, November 24, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 **Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005**
MySQL AB MySQL 3.x, 4.x	Two vulnerabilities exist: a vulnerability exists due to an error in 'ALTER TABLE ... RENAME' operations because the 'CREATE/INSERT' rights of old tables are checked, which potentially could let a remote malicious user bypass security restrictions; and a remote Denial of Service vulnerability exists when multiple threads issue 'alter' commands against 'merge' tables to modify the 'union.' Updates available at: http://dev.mysql.com/downloads/mysql/ Debian: http://security.debian.org/pool/updates/main/m/mysql Trustix: http://http.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesoft.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ SuSE: ftp://ftp.suse.com/pub/suse Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** We are not aware of any exploits for these vulnerabilities.	MySQL Security Restriction Bypass & Remote Denial of Service CAN-2004-0835 CAN-2004-0837	Low/ Medium (Low if a DoS; and Medium if security restrictions can be bypassed)	Secunia Advisory, SA12783, October 11, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:892, November 18, 2004 Ubuntu Security Notice, USN-32-1, November 25, 2004 SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 **Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005**

MySQL MySQL 4.x	A vulnerability exists in the 'mysqlaccess.sh' script because temporary files are created in an unsafe manner, which could let a malicious user obtain elevated privileges. Update available at: http://lists.mysql.com/internals/20600 Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-63-1 Debian: http://www.debian.org/security/2005/dsa-647 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-33.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** Currently we are not aware of any exploits for this vulnerability.	MySQL 'mysqlaccess.sh' Unsafe Temporary Files CAN-2005-0004	Medium	Security Tracker Alert, 1012914, January 17,2005 Ubuntu Security Notice USN-63-1 January 18, 2005 Debian Security Advisory DSA-647-1 mysql, January 19, 2005 Gentoo GLSA 200501-33, January 23, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:036, February 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 **Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005**
openMosixview openMosixview 1.2-1.5	Multiple vulnerabilities have been reported due to the creation of various temporary files that contain predictable filenames, which could let a malicious user create/overwrite arbitrary files. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	OpenMosixview Multiple Insecure Temporary File Creation CAN-2005-0894	Medium	Securiteam, March 28, 2005
SpamAssassin.org SpamAssassin prior to 2.64	A Denial of Service vulnerability exists in SpamAssassin. A a remote user can send an e-mail message with specially crafted headers to cause a Denial of Service attack against the SpamAssassin service. Update to version (2.64), available at: http://old.spamassassin.org/released/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/ Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-451.html **FedoraLegacy:** **http://download.fedoralegacy.org/fedora/** We are not aware of any exploits for this vulnerability.	SpamAssassin Remote Denial of Service CAN-2004-0796	Low	Security Tracker: 1010903, August 10, 2004 Mandrake Security Advisory, MDKSA-2004:084, August 19, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.041, September 15, 2004 Conectiva Linux Security Announcement, CLA-2004:867, September 22, 2004 RedHat Security Advisory, RHSA-2004:451-05, September 30, 2004 **Fedora Legacy Update Advisory, FLSA:2268 , March 24, 2005**
WebAPP WebAPP 0.9.9 .2, 0.9.9	A vulnerability has been reported due to an unspecified error, which could let a remote malicious user obtain sensitive information. Update available at: http://sourceforge.net/project/s... id=148219&release_id=316038 An exploit script has been published.	WebAPP Information Disclosure CAN-2005-0927	Medium	Secunia Advisory, SA14716, March 29, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Adventia E-Data 2.0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input when adding a new user to the directory, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Adventia E-Data Cross-Site Scripting CAN-2005-0924	High	Secunia Advisory: SA14739, March 29, 2005
All Enthusiast, Inc. PhotoPost PHP Pro 5.x	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in 'showgallery.php' due to insufficient sanitization of the 'password' and 'sort' parameters and in the 'slideshow.php' script due to insufficient sanitization of the 'photo' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported in 'showmembers.php' due to insufficient sanitization of the 'sl' parameter, which could let a remote malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploit scripts have been published.	PhotoPost PHP Pro Cross-Site Scripting & SQL Injection CAN-2005-0928 CAN-2005-0929	High	Secunia Advisory, SA14742, March 29, 2005
BirdBlog BirdBlog 1.0.0, 1.1.0	A vulnerability has been reported in 'admincore.php' due to insufficient sanitization of the 'userid' and 'userpw' parameters, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://birdblog.sourceforge.net/ There is no exploit code required.	BirdBlog 'AdminCore.PHP' Arbitrary SQL Injection CAN-2005-0882	High	Security Focus, 12880, March 23, 2005
Chatness Chatness 2.5, 2.5.1	A vulnerability has been reported in various chat message form fields, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Chatness Message Form Field Arbitrary Code Execution CAN-2005-0930	High	Security Focus, 12929, March 29, 2005
CPG-Nuke Dragonfly 9.0.2.0	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of several scripts, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	CPG Dragonfly Cross-Site Scripting CAN-2005-0914	High	Security Tracker Alert, 1013573, March 28, 2005
Deplate Deplate prior to 0.7.2	A vulnerability has been reported in the 'elements.rb' script due to insufficient validation of user-supplied ID values. The impact was not specified. Update available at: http://sourceforge.net/project/showfiles.php?group_id=108085 Currently we are not aware of any exploits for this vulnerability.	Deplate Input Validation CAN-2005-0912	Not Specified	Security Tracker Alert, 1013555, March 24, 2005
DigitalHive DigitalHive 2.0	A Cross-Site Scripting vulnerability has been reported in 'Base.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	DigitalHive 'Base.PHP' Cross-Site Scripting CAN-2005-0883 CAN-2005-0884	High	Security Focus, 12883, March 23, 2005
dream4 Koobi CMS 4.2.3	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'area' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Dream4 Koobi CMS 'Index.PHP' Cross-Site Scripting CAN-2005-0889 CAN-2005-0890	High	Secunia Advisory, SA14696, March 25, 2005

Ethereal Group Ethereal 0.10-0.10.8	A buffer overflow vulnerability exists due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Exploit scripts have been published.	Ethereal Buffer Overflow CAN-2005-0699	High	Security Focus, 12759, March 8, 2005 Security Focus, 12759, March 14, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005 RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005 **Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005** **ALTLinux Security Advisory, March 29, 2005**
Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the Etheric dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability has been reported in the GPRS-LLC dissector if the 'ignore cipher bit' option is enabled; a buffer overflow vulnerability has been reported in the 3GPP2 A11 dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and remote Denial of Service vulnerabilities have been reported in the JXTA and sFLow dissectors. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** A Denial of Service Proof of Concept exploit script has been published.	Ethereal Etheric/ GPRS-LLC/IAPP/ JXTA/s Flow Dissector Vulnerabilities CAN-2005-0704 CAN-2005-0705 CAN-2005-0739	Low/ HIgh (High if arbitrary code can be executed)	Ethereal Advisory, enpa-sa-00018, March 12, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005 RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005 **Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005** **ALTLinux Security Advisory, March 29, 2005**
exoops.info eXoops	Multiple input validation vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in the 'modules/newbb/viewforum.php' script due to insufficient sanitization of the 'sortdays' parameter and in the 'modules/newbb/index.php' script due to insufficient sanitization of the 'viewcat' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported in 'modules/newbb/index.php' script due to insufficient sanitization of the viewcat' parameter before used in an SQL query and in the 'modules/sections/index.php' script due	EXoops Multiple Input Validation CAN-2005-0910 CAN-2005-0911	High	Security Tracker Alert, 1013566, March 27, 2005

	to insufficient sanitization of the 'artid' parameter before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.			
IBM iSeries Server	A vulnerability has been reported in the AS/400 default configuration because user profiles are mapped to entries in the LDAP directory tree, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	AS/400 LDAP Server Default Configuration CAN-2005-0899	Medium	Security Tracker Alert, 1013571, March 28, 2005
Interspire ArticleLive 2005	A Cross-Site Scripting vulnerability has been reported in 'articles.newcomment' due to insufficient sanitization of the 'ArticleId' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	InterSpire ArticleLive NewComment Cross-Site Scripting CAN-2005-0881	High	Secunia Advisory, SA14708, March 23, 2005
Invision Power Services Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2, 1.3 Final, 1.3, 1.3.1, 2.0 PF1 & PF2, 2.0 PDR3, 2.0 Alpha 3, 2.0, 2.0.1, 2.0.2	A vulnerability has been reported due to insufficient sanitization of user-supplied data when filtering HTML tags, which could let a remote malicious user inject arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Power Board HTML Injection CAN-2005-0886	High	Security Focus, 12888, March 23, 2005
Jimmy <wordx@hotmail.com> The Includer 1.0, 1.1	A file include vulnerability has been reported which could let a remote malicious user execute arbitrary script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	The Includer Remote File Include CAN-2005-0931	High	Security Focus, 12926, March 29, 2005
MagicScripts E-Store Kit-2 PayPal Edition	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported because a remote malicious user can include a malicious PHP script which could lead to the execution of arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	MagicScripts E-Store Kit-2 PayPal Edition Cross-Site Scripting & Remote File Include CAN-2005-0897 CAN-2005-0898	High	Dcrab 's Security Advisory, March 25, 2005
MercuryBoard MercuryBoard Message Board 1.0-1.0.2, 1.1-1.1.2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'title' field when processing a private message, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.mercuryboard.com/index.php?a=downloads There is no exploit code required.	MercuryBoard 'Title' Field Cross-Site Scripting CAN-2005-0878	High	Secunia Advisory: SA14679, March 23, 2005
Michael Dean Double Choco Latte 0.9.3, 0.9.4 .3, 0.9.4.2, 0.9.4	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported due to an unspecified error, which could let a remote malicious user execute arbitrary PHP code. Upgrades available at: http://prdownloads.sourceforge.net/dcl/dcl-0.9.4.4.tar.gz?download There is no exploit code required.	Double Choco Latte Multiple Vulnerabilities CAN-2005-0887 CAN-2005-0888	High	Secunia Advisory, SA14688, March 24, 2005

Mozilla Mozilla 1.7.x and prior Mozilla Firefox 1.x and prior Mozilla Thunderbird 1.x and prior	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system. Firefox: Update to version 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.6 version. Thunderbird: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.0.1 version. Fedora update for Firefox: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-30.xml** **http://security.gentoo.org/glsa/glsa-200503-32.xml** **Slackware:** **http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla / Firefox / Thunderbird Multiple Vulnerabilities CAN-2005-0255 CAN-2005-0584 CAN-2005-0585 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593	High	Mozilla Foundation Security Advisories 2005-14, 15, 17, 18, 19, 20, 21, 24, 28 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005 **Fedora Update Notification, FEDORA-2005-248, 249, 251, & 253, March 23 & 25, 2005** **Gentoo Linux Security Advisory, GLSA 200503-30 & GLSA 200503-032, March 25, 2005** **Slackware Security Advisory, SSA:2005-085-01, March 27, 2005**
Mozilla.org Firefox prior to 1.0.2	A vulnerability has been reported if a malicious web page is bookmarked as a sidebar panel, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Currently we are not aware of any exploits for this vulnerability.	Mozilla Firefox Sidebar Panel Script Injection CAN-2005-0402	High	Mozilla Foundation Security Advisory 2005-31, March 23, 2005
Mozilla.org Mozilla Suite prior to 1.7.6, Firefox prior to 1.0.2	A vulnerability has been reported when processing drag and drop operations due to insecure XUL script loading, which could let a remote malicious user execute arbitrary code. Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ Firefox: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa	Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution CAN-2005-0401	High	Mozilla Foundation Security Advisory 2005-32, March 23, 2005

	/glsa-200503-30.xml http://security.gentoo.org /glsa/glsa-200503-31.xml Slackware: http://slackware.com/security/ viewer.php?l=slackware-security &y=2005&m=slackware-security. 000123 A Proof of Concept exploit has been published.			
Mozilla.org Firefox 1.x, 0.x, Mozilla 1.7.x, 1.6, 1.5, 1.4, 1.3, 1.2, 1.1, 1.0, 0.x	A vulnerability exists because a website can inject content into another site's window if the target name of the window is known, which could let a remote malicious user spoof the content of websites Gentoo: http://security.gentoo.org/ glsa/glsa-200503-10.xml **Fedora:** **http://download.fedora.redhat.** **com/pub/fedora/linux/** **core/updates/** **Gentoo:** **http://security.gentoo.org/** **glsa/glsa-200503-30.xml** **Slackware:** **http://slackware.com/security/** **viewer.php?l=slackware-security** **&y=2005&m=slackware-security** **.000123** A Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.	Mozilla Browser and Mozilla Firefox Remote Window Hijacking CAN-2004-1156	Medium	Secunia SA13129, December 8, 2004 Gentoo Linux Security Advisory GLSA 200503-10, March 4, 2005 **Fedora Update Notifications, FEDORA-2005-248 & 249,** **2005-03-23** **Fedora Update Notifications, FEDORA-2005-251 & 253, March 25, 2005** **Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005** **Slackware Security Advisory, March 28, 2005**
Mozilla.org Mozilla Browser Suite prior to 1.7.6 ; Thunderbird prior to 1.0.2 ; Firefox prior to 1.0.2	A buffer overflow vulnerability has been reported due to a boundary error in the GIF image processing of Netscape extension 2 blocks, which could let a remote malicious user execute arbitrary code. Mozilla Browser Suite; http://www.mozilla.org/products/ mozilla1.x/ Thunderbird: http://download.mozilla.org/? product=thunderbird-1.0.2& os=win(=en-US Firefox: http://www.mozilla.org/products/ firefox/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/ Slackware: http://slackware.com/security/ viewer.php?l=slackware-security &y=2005&m=slackware-security. 000123 Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite/ Firefox/ Thunderbird GIF Image Processing Remote Buffer Overflow CAN-2005-0399	High	Mozilla Foundation Security Advisory 2005-30, March 23, 2005
Mozilla Firefox 1.0	A vulnerability exists in the XPCOM implementation that could let a remote malicious user execute arbitrary code. The exploit can be automated in conjunction with other reported vulnerabilities so no user interaction is required. A fixed version (1.0.1) is available at: http://www.mozilla.org/products/ firefox/all.html Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ **Gentoo:** **http://security.gentoo.org/**	Mozilla Firefox Remote Code Execution Vulnerability CAN-2005-0527	High	Security Tracker Alert ID: 1013301, February 25, 2005 Gentoo Linux Security Advisory GLSA 200503-30. March 25, 2005

	glsa/glsa-200503-30.xml A Proof of Concept exploit has been published.			
Mozilla Mozilla 0.x, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7.x Mozilla Firefox 0.x Mozilla Thunderbird 0.x	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird that can permit users to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Mozilla: Update to version 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Firefox: Update to version 1.0: http://www.mozilla.org/products/firefox/ Thunderbird: Update to version 1.0: http://www.mozilla.org/products/thunderbird/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Slackware:** **http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities CAN-2005-0141 CAN-2005-0143 CAN-2005-0144 CAN-2005-0145 CAN-2005-0146 CAN-2005-0147 CAN-2005-0148 CAN-2005-0149 CAN-2005-0150	Medium/ High (High if arbitrary code can be executed)	Mozilla Foundation Security Advisory 2005-01, 03, 04, 07, 08, 09, 10, 11, 12 **Fedora Update Notification, FEDORA-2005-248, 249, 251, 253, March 23 & 25, 2005** **Slackware Security Advisory, SSA:2005-085-01, March 27, 2005**
Mozilla Mozilla Firefox 1.0 and 1.0.1	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-30.xml** A Proof of Concept exploit has been published.	Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability CAN-2005-0591	High	Secunia SA14406, March 1, 2005 **Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005**
Multiple Vendors Instance Four Tincat Release 2; Sacred Sacred 1.8.2 .6; UBI Soft The Settlers: Heritage of Kings 1.0 2	A buffer overflow vulnerability has been reported in the function responsible for logging users to a game server, which could let a remote malicious user obtain unauthorized access. game server. Please contact the vendors to obtain the fixed versions. A Proof of Concept exploit script has been published.	Tincat Network Library Remote Buffer Overflow CAN-2005-0906	Medium	Security Focus, 12912, March 28, 2005
Multiple Vendors Mozilla Firefox 1.0; Gentoo Linux; Thunderbird 0.6, 0.7- 0.7.3, 0.8, 0.9, 1.0, 1.0.1; Netscape Netscape 7.2	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository Fedora: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win<=en-US **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-30.xml** A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	Security Tracker Alert ID: 1013108, February 8, 2005 Fedora Update Notification, FEDORA-2005-182, February 26, 2005 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 Security Focus, 12468, March 22, 2005 **Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005**
Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4,	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted,	Telnet Client 'slc_add_reply()' & 'env_opt_add()'	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924

10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386	which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/ Currently we are not aware of any exploits for these vulnerabilities.	Buffer Overflows CAN-2005-0468 CAN-2005-0469		
Multiple Vendors Check Point Software FireWall-1 R55 HFA08 with SmartDefense; Internet Security Systems SiteProtector 2.0.4.561, 2.0 SP3; IronPort IronPort with Sophos AV Engine 3.88; McAfee Webshield 3000 4.3.20; TippingPoint Unity-One with Digital Vaccine 2.0.0.2070; Trend Micro InterScan Messaging Security Suite 3.81, 5.5, Trend Micro WebProtect 3.1	A security vulnerability exists due to a failure to decode base64-encoded images in 'data' URIs, which could lead to a false sense of security. Gentoo: http://security.gentoo.org/glsa/glsa-200501-46.xml Mandrake: http://www.mandrakesoft.com/security/advisories **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** There is no exploit required.	Multiple Vendor Anti-Virus Gateway Base64 Encoded Image Decode Failure CAN-2005-0218	Medium	Bugtraq, January 11, 2005 **ALTLinux Security Advisory, March 29, 2005**

Multiple Vendors Debian Linux 3.0 spar, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.7	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the DICOM dissector; a remote Denial of Service vulnerability exists in the handling of RTP timestamps; a remote Denial of Service vulnerability exists in the HTTP dissector; and a remote Denial of Service vulnerability exists in the SMB dissector when a malicious user submits specially crafted SMB packets. Potentially these vulnerabilities may also allow the execution of arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200412-15.xml Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-011.html SuSE: ftp://ftp.suse.com/pub/suse/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Denial of Service & Potential Code Execution Vulnerabilities CAN-2004-1139 CAN-2004-1140 CAN-2004-1141 CAN-2004-1142	Low/High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00016, December 15, 2004 Conectiva Linux Security Announcement, CLA-2005:916, January 13, 2005 RedHat Security Advisory, RHSA-2005:011-11, February 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 **ALTLinux Security Advisory, March 29, 2005**
Multiple Vendors OpenPGP	A vulnerability exists that could permit a remote malicious user to conduct an adaptive-chosen-ciphertext attack against OpenPGP's cipher feedback mode. The flaw is due to an ad-hoc integrity check feature in OpenPGP. A solution will be available in the next release of the product. SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandrake: http://www.mandrakesecure.net/en/ftp.php **Gentoo: http://security.gentoo.org/glsa/glsa-200503-29.xml** **ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** A Proof of Concept exploit has been published.	Multiple Vendors OpenPGP CFB Mode Vulnerable to Cipher-Text Attack CAN-2005-0366	Medium	US-CERT VU#303094 SUSE Security Summary Report, SUSE-SR:2005:007, March 4, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:057, March 16, 2005 **Gentoo Linux Security Advisory, GLSA 200503-29, March 24,2005** **ALTLinux Security Advisory, March 29, 2005**
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability was reported in the CREATE FUNCTION command that could let an authenticated user gain mysql user privileges on the target system and permit the user to execute arbitrary code. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/	MySQL CREATE FUNCTION Remote Code Execution Vulnerability CAN-2005-0709	High	Security Tracker Alert ID: 1013415, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 **SUSE Security**

	trustix/updates/ **ALT Linux:** **http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-334.html** **SuSE:** **ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published.			**Announcement, SUSE-SA:2005:019, March 24, 2005** **RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005** **ALTLinux Security Advisory, March 29, 2005**
NetComm NB1300, NB1300 4.4.1	A remote Denial of Service vulnerability has been reported when attempting to use a ping or other ICMP floods. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Netcomm NB1300 Modem/Router Remote Denial of Service CAN-2005-0895	Low	Securiteam, March 28, 2005
Nuke Bookmarks Nuke Bookmarks 0.6	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability has been reported in 'modules.php' due to insufficient sanitization of the 'category' parameter, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability has been reported in the 'marks.php' file, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://prdownloads.sourceforge.net/nukebookmarks/bookmarks-0.7.tgz?download There is no exploit code required; however, Proofs of Concept exploits have been published.	Nuke Bookmarks Multiple Remote Vulnerabilities CAN-2005-0900 CAN-2005-0901 CAN-2005-0902	Medium/ High (High if arbitrary code can be executed)	ZH2005-03SA Advisory, March 26, 2005
OpenGroupware.org SOGo	A vulnerability has been reported which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	SOGo Information Disclosure CAN-2004-1771	Medium	Security Tracker Alert, 1013553, March 24, 2005
Oracle Corporation Oracle Reports 10g 9.0.4 .3.3	Multiple Cross-Site Scripting vulnerabilities have been reported which due to insufficient sanitization of user-supplied input, could let al remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Oracle Reports Server 10g Multiple Remote Cross-Site Scripting CAN-2005-0873	High	Security Focus, 12892, March 24, 2005
PHP Group PHP 4.3.6-4.3.9, 5.0 candidate 1-canidate 3, 5.0 .0-5.0.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'pack()' function, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the 'unpack()' function, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'safe_mode' when executing commands, which could let a remote malicious user bypass the security restrictions; a vulnerability exists in 'safe_mode' combined with certain implementations of 'realpath(),' which could let a remote malicious user bypass security restrictions; a vulnerability exists in 'realpath()' because filenames are truncated; a vulnerability exists in the 'unserialize()' function, which could let a remote malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists in the 'shmop_write()' function, which may result in an attempt to write to an out-of-bounds memory location; a vulnerability exists in the 'addslashes()' function because '\0' if not escaped correctly; a vulnerability exists in the 'exif_read_data()' function when a long sectionname is used, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in 'magic_quotes_gpc,' which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.php.net/downloads.php Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva:	PHP Multiple Remote Vulnerabilities CAN-2004-1018 CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020 CAN-2004-1065	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 16, 2004 Conectiva Linux Security Announcement, CLA-2005:915, January 13, 2005 Red Hat, Advisory: RHSA-2005:031-08, January 19, 2005 SUSE Security Announcement, SUSE-SA:2005:002, January 17, 2005 Ubuntu Security Notice, USN-66-1, January 20, 2005 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 Ubuntu Security Notice,

	ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-031.html SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Apple: http://www.apple.com/support/downloads/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/php4/** There is no exploit code required; however, a Proof of Concept exploit script has been published.			USN-99-1 March 18, 2005 **Ubuntu Security Notice, USN-99-2 March 24, 2005**
phpCOIN phpCOIN 1.2, 1.2.1 b, 1.2.1	Multiple input validation vulnerabilities have been reported including multiple SQL injection vulnerabilities and a file include vulnerability which could let a remote malicious user manipulate/view arbitrary database contents and execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPCoin Multiple Remote Vulnerabilities CAN-2005-0932 CAN-2005-0933	Medium/ High (High if arbitrary code can be executed)	Security Focus, 12917, March 29, 2005
phpMyDirectory phpMyDirectory 10.1.3 -rel	A Cross-Site Scripting vulnerability has been reported in the 'review.php' script in the 'subcat,' 'page,' 'subsubcat' variables, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPMyDirectory 'Review.PHP' Cross-Site Scripting CAN-2005-0896	High	Talte Security Advisory #3, March 25, 2005
phpSysInfo phpSysInfo 2.3	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. It is also possible to obtain the full path to certain scripts. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPSysInfo Multiple Cross-Site Scripting CAN-2005-0870	High	Secunia Advisory, SA14690, March 24, 2005
PowerDev Team EncapsBB 0.3.2_fixed	A vulnerability has been reported in 'index_header.php' due to insufficient validation of the 'root' parameter, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	EncapsBB Remote Arbitrary Command Execution CAN-2005-0917	High	[In]Security Research 2005-003, March 26, 2005
Ptirhiik Topic Calendar 1.0.1	A Cross-Site Scripting vulnerability has been reported in the 'calendar_scheduler.php' script due to insufficient validation of the 'start' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Topic Calendar 'Calendar_ Scheduler. PHP' Cross-Site Scripting CAN-2005-0872	High	CODEBUG Labs Advisory #8, March 24, 2005
smarty.php.net prior to 2.6.8	A vulnerability has been reported in 'libs/plugins/modifier.regex_replace.php' due to insufficient validation of the 'search' parameter, which could let a malicious user execute PHP code. Update available at: http://smarty.php.net/download.php Currently we are not aware of any exploits for this vulnerability.	Smarty 'regex_replace' Modifier Template Arbitrary PHP Code Execution CAN-2005-0913	High	Security Tracker Alert, 1013556, March 24, 2005

SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml Conectiva: ftp://atualizacoes.conectiva.com.br/9 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Apple: http://www.apple.com/support/downloads/ SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://www.debian.org/security/2005/dsa-662 Red Hat: http://rhn.redhat.com/errata/RHSA-2005-135.html Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** An exploit script is not required.	SquirrelMail Cross-Site Scripting CAN-2004-1036 CAN-2005-0104 CAN-2005-0152	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 Fedora Update Notifications, FEDORA-2004-471 & 472, November 28, 2004 Conectiva Linux Security Announcement, CLA-2004:905, December 2, 2004 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 Debian DSA-662-1, February 1, 2005 Red Hat RHSA-2005:135-04, February 10, 2005 Debian Security Advisory, DSA 662-2, March 14, 2005 **Fedora Update Notifications FEDORA-2005-259 & 260, March 28, 2005**
The XMB Group XMB Forum 1.9.1	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	XMB Forum Multiple Remote Cross-Site Scripting CAN-2005-0885	High	Security Focus, 12886, March 23, 2005
TKai's Shoutbox TKai's Shoutbox	A URI redirection vulnerability has been reported in the 'query' parameter, which could let a remote malicious user steal cookie based authentication credentials. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Tkai's Shoutbox Query Parameter URI Redirection CAN-2005-0909	Medium	Security Focus, 12914, March 28, 2005
Valdersoft Shopping Cart 3.0	Several vulnerabilities have been reported: a vulnerability has been reported in the 'category.php,' 'item.php,' 'index.php,' and 'search_result.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability has been reported due to insufficient filtering of HTML code from various scripts, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Valdersoft Shopping Cart Multiple Input Validation CAN-2005-0907 CAN-2005-0908	High	Dcrab 's Security Advisory, March 27, 2005
Vortex Portal Vortex Portal 2.0	A vulnerability has been reported in 'content.php' and 'index.php' due to insufficient sanitization of the 'act' parameter before used to include files, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a	Vortex Portal Remote 'Content.php' File Include CAN-2005-0879	High	Secunia Advisory, SA14707, March 24, 2005

	Proof of Concept exploit has been published.			
WackoWiki WackoWiki R4	Multiple Cross-Site scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://wackowiki.com/WackoDownload/InEnglish#h4828-8 There is no exploit code required.	WackoWiki Multiple Cross-Site Scripting CAN-2005-0934	High	Secunia Advisory, SA14720, March 29, 2005
Webmasters-Debutants WD-Guestbook 2.8	A vulnerability has been reported in the '/admin/valid/ajout_admin2.php' script due to insufficient authentication, which could let a remote malicious user modify system/user information. Update available at: http://www.webmasters-debutants.com/clic/telecharge.php?id=2ZDQ624lZz3 A Proof of Concept exploit has been published.	WD Guestbook Authentication Error CAN-2005-0915	Medium	Security Tracker Alert, 1013570, March 28, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
March 29, 2005	answerbook2.txt	Yes	Exploit for the Sun Answerbook2 Cross-Site Scripting vulnerability.
March 29, 2005	blackmagic.txt	N/A	A guide to advanced network attack and reconnaissance techniques using Python. Includes topics such as firewalking, port scanning, ARP poisoning, and DNS poisoning.
March 29, 2005	photopostSQLXSS.txt	No	Detailed exploitation for the PhotoPost PHP Pro Cross-Site Scripting & SQL Injection vulnerabilities.
March 29, 2005	smack.c.gz	No	Exploit for the Smail-3 Remote preparse_address_1() heap buffer overflow vulnerability.
March 29, 2005	vladersoft30.txt	No	Sample exploitation for the Valdersoft Shopping Cart Multiple Input Validation vulnerabilities.
March 29, 2005	WepDecrypt-0.5.tar.gz	N/A	A wireless LAN tool based on wepattack that guesses WEP keys using an active dictionary attack, a key generator, a distributed network attack, and some other methods.
March 28, 2005	dcrab-e-xoops.txt	No	Proof of Concept URLs for the EXoops Multiple Input Validation vulnerabilities.
March 28, 2005	kernelBluetoothSocketPoC.c	Yes	Proof of Concept exploit for the Linux Kernel Bluetooth Signed Buffer Index Vulnerability.
March 28, 2005	relayscanner.zip	N/A	SMTP relay scanner that checks for open relays and misconfigurations that allow spoofing via the tested mailserver or for internal mail to internal address from external nets.
March 28, 2005	RX_oMcollector_proof.sh dvRX250305.txt	No	Proof of Concept exploits for the OpenMosixview Multiple Insecure Temporary File Creation vulnerabilities.
March 28, 2005	timbuktu_userbrute.c	N/A	Timbuktu Pro Remote Control user enumeration program is a wordlist-based bruteforce tool that checks whether a given username exists on the target server or not, which is possible due to a difference in the error message returned when the username is invalid versus when the password is invalid.
March 28, 2005	tincat2bof.zip	Yes	Proof of Concept exploit for the Tincat Network Library Remote Buffer Overflow vulnerability.
March 28, 2005	ZH2005-03SA.txt	Yes	Example URLs for the Nuke Bookmarks Multiple Remote Vulnerabilities.
March 25, 2005	cachedump-1.1.zip	N/A	CacheDump is a tool that demonstrates how to recover cache entry information: username and hashed password (called MSCASH). This tool also explains the technical issues underneath Windows password cache entries, which are undocumented by Microsoft.
March 25, 2005	lameSeries60NokiaDoS.pl	No	An exploit for the Nokia/Symbian Series60 bluetooth device-name handling vulnerability.
March 25, 2005	phpbb2013user.txt	No	Exploit for the phpbb vulnerability.
March 25, 2005	WebApp_HTTPMod.pdf	N/A	A whitepaper that describes how the IHttpModule that comes with the .Net framework can be used to man-in-the-middle HTTP transactions in order to help filter against input validation attacks.
March 25, 2005	WebServices_Profiling.pdf	N/A	A whitepaper that discusses the scope of information gathering used against web services. Second in a series of papers defining attack and defense methodologies with web services.
March 24, 2005	Attack_5250_terminal_em.pdf	No	A paper that describes how insertion of commands inside an AS/400 application allows them to be executed as a command on the connected PC.
March 24, 2005	cisco-torch-0.4b.tar.bz2	N/A	Cisco Torch mass scanning, fingerprinting, and exploitation tool.

March 24, 2005	essus-installer-2.2.4.sh	N/A	A free, up-to-date, and full featured remote vulnerability scanner for Linux, BSD, Solaris and other systems.
March 24, 2005	snmp-fuzzer-0.1.1.tar.bz2	N/A	SNMP fuzzer uses Protos test cases with an entirely new engine written in Perl. It provides efficient methods of determining which test case has caused a fault, offers more testing granularity and a friendlier user interface. Happy vulnerability searching.
March 22, 2005	phpautolog.pl	No	phpBB versions 2.0.12 and below remote session autologin exploit that gives a user administrative rights.

[back to top]

Trends

- **Phishing Attacks Jump 26%**: According to the Anti-phising Working Group in the February Phishing Activity Trends report "Phishing without a lure" is an increasingly common attack style. The report, compiled with research from Websense Security Labs and Tumbleweed Message Protection Lab, reported 13,141 new, unique phishing e-mail messages in February 2005, more than a 2 percent increase over January. The average monthly growth rate in attacks since July 2004 was 26 percent. The United States continues to be the top location geographic location for hosting phishing sites with more than 37%, which was almost a 6% increase from last month. Source: http://www.internetnews.com/security/article.php/3493046. Report: http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf
- **First IM phishing attack hits Yahoo!**: The first phishing attack carried out via instant messenger tried to trick Yahoo Messenger users last week into giving up information that would let attackers access their IM account and contact list. Yahoo Messenger users have been spimmed (spam for IM) with messages that include a link to a bogus Web site that looks like an official Yahoo page, which asks them to log in with their Yahoo username and password. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=159906218
- **Experts debate real risk of cell phone viruses**: When anti-virus researchers reported the discovery of the first proof-of-concept cell phone virus, analysts and experts immediately predicted a coming wave of malware targeting high-end mobile devices. But not everyone is convinced that the risk is high enough to justify the investments. "A lot of this is hyped to create a market that doesn't exist," said Neil MacDonald, group vice president and research director at Gartner Inc. However, Kaspersky Labs, the well-known Russian anti-virus company has a different view. "Malware for smart phones is now evolving, and seems likely to become a growing threat as smart phones gain popularity," the company said in a statement. Symantec Corp., Trend Micro Inc. and McAfee Inc. also have invested in mobile anti-virus products. Source: http://www.eweek.com/article2/0,1759,1779359,00.asp.
- **High-profile identify thefts force government, industry to take action**: The Federal Trade Commission logged 635,000 consumer complaints for fraud and identity theft last year, with 61% for fraud and 39% for identity theft This rash of identity thefts has businesses and government agencies exploring new options for locking down resources and setting policies. Source: http://www.nwfusion.com/news/2005/032805-identity-theft.html?ts%A0
- **Hackers phishing for Chinese victims**: Chinese consumers are becoming increasingly popular targets of international Internet scammers, or "phishers", hoping to con the country's growing ranks of Web surfers out of their money. "China reported 223 fake Web sites last year, a huge increase from only one reported from 2002 to 2003," Source: http://www.expressindia.com/fullstory.php?newsid=43954.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Bagle-BJ	Win32 Worm	Stable	January 2005
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Netsky-Q	Win32 Worm	Stable	March 2004
5	Zafi-B	Win32 Worm	Stable	June 2004
6	Netsky-D	Win32 Worm	Stable	March 2004
7	Netsky-Z	Win32 Worm	Stable	April 2004
8	Netsky-B	Win32 Worm	Stable	February 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Bagle.BB	Win32 Worm	Stable	September 2004

Table Updated March 29, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Drever-C**: Malware authors have created a Trojan that targets Symbian smart phones and attempts to remove any anti-virus protection it finds. Drever-C poses as a security update and tries to damage the boot loader and application binaries of F-Secure Mobile Anti-Virus. Like all mobile malware threats to date, Drever-C is rare and largely a risk confined to people downloading content from disreputable sources. Source: http://www.theregister.co.uk/2005/03/23/mobile_trojan_targets_av/

- **Mytob**: Multiple variations of the Mytob worm have appeared in the last week, said Symantec, all of them able to plant a backdoor on infected machines and prevent them from updating security software. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=159907336

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Dextenea		Trojan
Backdoor.Fuwudoor		Trojan
Backdoor.Livehar		Trojan
Backdoor.Nibu.J		Trojan
BackDoor-CPG		Trojan
Downloader.BHV	Trj/Downloader.BHV Win32.Small.aow	Win32 Worm
Downloader-WY		Trojan
Mydoom.AQ	Email-Worm.Win32.Mydoom.aq	Win32 Worm
PWSteal.Ldpinch.E	Trojan-PSW.Win32.PdPinch.gen	Trojan
Skulls.G	SymbOS/Skulls.G	Symbian OS Worm
Skulls.H	SymbOS/Skulls.H	Symbian OS Worm
StartPage-GQ		Trojan
SYMBOS_COMWAR.B		Symbian OS Worm
SYMBOS_DREVER.B		Symbian OS Worm
SYMBOS_DREVER.C		Symbian OS Worm
SYMBOS_SKULLS.F		Symbian OS Worm
Troj/Bancos-BV	Trojan-Spy.Win32.Bancos.bg TROJ_BANCDROP.D	Trojan
Troj/Bdoor-FW	Backdoor.Win32.Agent.co BackDoor-BDI BKDR_BDI.A	Trojan
Troj/HideDial-E	Trojan-Downloader.Win32.Tibser.c Trojan.Downloader.Tibser-3	Trojan
Troj/PurScan-W	Trojan-Dropper.Win32.PurityScan.l	Trojan
TROJ_BANCOS.SM		Trojan
Trojan.Mochi		Trojan
W32.Clunk.A		Win32 Worm
W32.Elitper.E@mm		Win32 Worm
W32.Mytob.O@mm	WORM_MYTOB.O	Win32 Worm
W32.Mytob.R@mm		Win32 Worm
W32.Mytob.S@mm	WORM_MYTOB.S	Win32 Worm
W32.Reidana.A		Win32 Worm
W32/Agobot-RB		Win32 Worm
W32/Agobot-RC	Backdoor.Win32.Agobot.aal	Win32 Worm
W32/Agobot-RE		Win32 Worm
W32/BlackMagic.bat		Win32 Worm
W32/Catc-A		Win32 Worm
W32/Forbot-Gen		Win32 Worm
W32/Krynos-B	WORM_KRYNOS.B	Win32 Worm
W32/Mytob-D		Win32 Worm
W32/Mytob-E	Net-Worm.Win32.Mytob.h	Win32 Worm
W32/Mytob-G	W32/Mytob.gen@MM.b	Win32 Worm
W32/Mytob-H	IM-Worm.Win32.Prex.a	Win32 Worm
W32/Mytob-K		Win32 Worm
W32/Mytob-N	Net-Worm.Win32.Mytob.m W32/Mytob.N@mm Worm.Mytob.N	Win32 Worm
W32/Rbot-ZA	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.y WORM_SPYBOT.WV	Win32 Worm
W32/Sdbot.worm!184320		Win32 Worm
W32/Sdbot-WG	Backdoor.Win32.SdBot.gen	Win32 Worm
W32/Sdbot-WK		Win32 Worm

W32/Sdbot-WM	Backdoor.Win32.SdBot.un	Win32 Worm
Win32.Elitper.B		Win32 Worm
Win32.Elitper.C		Win32 Worm
Win32.Elitper.D		Win32 Worm
Win32.Seenbot.O		Win32 Worm
Win32.Seenbot.R		Win32 Worm
WORM_BUCHON.F		Win32 Worm
WORM_CROWT.C	W32/Crowt-C	Win32 Worm
WORM_ELITPER.E	W32.Elitper.E@mm W32/Generic.m W32/Wifil.worm!p2p Win32.Worm.P2P.Wif.A Win32/Unknown!P2P!Worm Worm:Win32/Elitper.E	Win32 Worm
WORM_ELITPER.E		Win32 Worm
WORM_KELVIR.I		Win32 Worm
WORM_MYDOOM.AE		Win32 Worm
WORM_MYTOB.I		Win32 Worm
WORM_MYTOB.J	W32.Mytob.J@mm	Win32 Worm
WORM_MYTOB.K	W32.Mytob.K@mm	Win32 Worm
WORM_MYTOB.L	W32.Mytob.L@mm	Win32 Worm
WORM_MYTOB.M	W32.Mytob.M@mm	Win32 Worm
WORM_MYTOB.N		Win32 Worm
WORM_MYTOB.P	Win32.Mytob.P	Win32 Worm
WORM_MYTOB.Q	W32.Mytob.Q@mm	Win32 Worm
X97M.Dropo		Word 97 Macro Virus

[back to top]

Last updated March 30, 2005